基于 SecOC 的车载网络通信安全模型研究 *

章 意，李 飞†，张森葳

(成都信息工程大学 网络空间安全学院，成都 610200)

摘 要：车载电子设备的增加使得车载网络面对越来越多的威胁。车载网络中电子控制单元(Electronic Control Unit，ECU)无认证、控制器局域网络(Controller Area Network，CAN)通信数据无加密等缺陷使得车载网络易遭受重放、ECU 注入、中间人伪造消息、窃听等恶意攻击，造成严重后果。针对现在的车载网络威胁现提出一种基于 SecOC 的车载网络安全通信模型，该模型使用 SM4 的密码算法与基于 Bkake2s 的改进密钥管理，实现车载 ECU 的认证和车载网络消息的加密与认证。最后经过分析与测试，该模型可以保护车载网络安全并更高效。

关键词：板端加密通信；车载网络；SM4；Blake2s；PBKDF2；硬件安全模块

中图分类号：TP39　　doi: 10.19734/j.issn.1001-3695.2021.12.0703

Research on security model of vehicle network communication based on SecOC

Zhang Yi, Li Fei†, Zhang Senwei

(*School of Cyberspace Security*, *Chengdu University of information engineering*, *Chengdu* 610200, *China*)

Abstract: The increase of in-vehicle electronic equipment makes the in-vehicle network face more and more threats. The lack of authentication of the Electronic Control Unit in the in-vehicle network and the lack of encryption of the communication data of the Controller Area Network make the in-vehicle network vulnerable to replay, ECU injection, man-in-the-middle forged messages, eavesdropping, etc, Witch make serious consequences. Aiming at the current vehicle network threats, a vehicle network security communication model based on SecOC is proposed. This model uses the SM4 cryptographic algorithm and the improved key management based on Bkake2s to realize the authentication of the vehicle ECU and the encryption and authentication of the vehicle network message. Finally, after analysis and testing, the model can protect the in-vehicle network security and be more efficient.

Key words: security onboard communication; in-vehicle network; SM4; Blake2s; password-based key derivation function 2; hardware security moduel

0 引言

车端威胁复杂，涉及众多车载组件，文献[1]中阐述了 CAN 和 ECU 存在的多种安全漏洞，车载网络在攻击方式多样化的如今成为首当其冲的薄弱点。

2016 年，汽车开放系统架构 4.3(AUTomotive open system architecture，AUTOSAR) 标准中提出了 SecOC 用于提高 PDU(protocal data unit)上关键数据的安全性，保护 ECU 通信[2]。SecOC 的细节将在 1.1 节说明。此后，国内外学者关于 SecOC 模块的研究尚处于初步探索阶段。

国内的研究中，文献[3~8]都实现了 SecOC 模块中的 ECU 通信。吴志红等人[4]基于 CMAC 实现 MAC 认证，但没有细节说明数据帧的格式；罗峰[5]使用会话密钥加密通信消息，但 ECU 需要保管多个密钥并不安全；黄大权[6]将会话密钥初始化写入 ECU，造成 ECU 存储压力且密钥易丢失；罗超[7]基于 CAMC-AES 截取 16 位的 MAC 码，安全性有限，且根据数据帧信息动态从本地密钥库更新会话密钥会造成额外的计算开销，延迟通信；刘毅[8]实现了车载 CAN 通信的认证与加密，但 ECU 存储与计算压力都超过现有框架。

国外对于车载网络的安全通信研究较早，在 SecOC 尚未推出时，已有学者设计了符合 AUTOSAR 架构的安全通信模型。Böhner 等人[9]扩展了 AES 用于数据加密，但是并没有具体描述模型的流程，并且软件形式的保护不完善，缺乏密钥管理；Radu 等人[10]提出了一种 CAN 认证协议 LeiA，使用派生的会话密钥实现 ECU 间身份认证，但是两两认证易使车载通信时效低，ECU 需要保存消息 ID 对应的长期密钥，这存在泄露风险；Nyurnberger 等人[11]设计了一种 vatiCAN 模型使用长期密钥验证消息，但固定密钥并不是安全策略，且周期性的新鲜度值更新存在概率重放攻击漏洞。Jo 等人[12]在文献[10,11]的基础上提出 VulCAN，但其 MAC 验证需要加倍的通信量，消息 ID 与会话密钥绑定验证的方式使得密钥管理复杂。

待到 SecOC 出现后，Wu 等人[13]在 SecOC 中使用 2 字节的新鲜度值和 2 字节的基于 AES 的 MAC 认证码；Rosenstatter[14,15]对于官方 SecOC 的 Profile 3 进行了一定的修改，在其基础上提出了 Profile 4，但增加了车载网络的通信负担，易引起混乱；Bellad 等人[16]将 CINNAMON 作为 SecOC 模块的继承与扩展，实现数据的加密，但是密码管理不清晰；Yang 等人[17]设计了 KDC 风格的密钥分发协议 SKDC，但方案中 ECU 存储和计算压力过大；Yalcin 等人[18]在硬件中实现 AES 算法与 SecOC 的 E2E 安全通信，但密钥存在遗失风险。

可见基于 SecOC 的安全模型虽然实现了消息认证与验证，但依然存在以下问题需要解决：

a) 明文传输，不能防窃取和中间人攻击。
b) 会话密钥缺乏安全地管理。
c) 通信 ECU 缺乏有效认证手段。
d) 保证安全性时，通信效率有待提升。

本研究基于 SecOC 设计一种车载网络安全通信模型：首

收稿日期：2021-12-14；**修回日期：**2022-03-14　**基金项目：**四川省重大科技专项课题(18ZDZX0013)；四川省科技重点研发项目(19ZDYF0789)

作者简介：章意(1997-)，男，江苏无锡人，硕士研究生，主要研究方向为车联网安全、网络安全；李飞(1966-)，男(通信作者)，湖南常德人，教授，硕导，硕士，主要研究方向为车联网安全，网络安全(lifei@cuit.edu.cn)；张森葳(1998-)，男，四川绵阳人，硕士研究生，主要研究方向为车联网安全.

先根据汽车安全完整性等级(Automotive Safety Integrity Level，ASIL)将 ECU 划分安全等级，其次在点火阶段使用 Blake2s 改进的 PBKDF2 算法来计算会话密钥，接着再通信阶段使用 SM4 加密解密通信数据、Blake2s 计算验证 MAC，最后分析并验证模型的安全性与效率。

1　相关知识

1.1　SecOC

SecOC[2]提供完整性与真实性保障的 Secured I-PDU，它包含一个 Authentic I-PDU，Freshness Value 以及 Authentictor，如图 1 所示，其中 Authentic I-PDU 是一个任意的 AUTOSAR I-PDU，Authentictor 是消息认证码 MAC 或者签名，Freshness Value 是新鲜度值，分为计数器或时间戳两种。

Secured I-PDU Header	Authentic I-PDU	Freshness value	Authenticor

图 1　Secured I-PDU 结构图

Fig. 1　Structure diagram of secured i-pdu

1.2　HSM

硬件安全模块(Hardware Security Module，HSM)是一个用于管理密钥和提高数据加解密处理速度的物理计算设备，通常形为插入式卡片或外接设备，能够为数据提供安全性保障[19]。硬件安全模块提供比软件更高级别的安全，具有不可复制性，抗渗透性，抗非法的连接及窜改。所以使用 HSM 可以更快地计算的同时，也可以提供更高的安全性，并且硬件安全模块在设计之初，作为一种外接式设备，天生适合现在的车联网环境。例如欧洲资助的项目之一，EVITA 为车载网络安全开发了 HSM 模块，HSM 采用专用硬件实现，优化固件之后，计算速度快于软件，具有低延迟，高性能和节约成本的特点。本研究中使用已经写入算法并优化固件的 HSM 完成相关计算。

1.3　CAN-FD

CAN-FD(CAN with Flexible Data-Rate)是 BOSCH 推出的 CAN 改进版，可支持最高 64 字节长度的数据载荷，并且可调速率最高达 8Mbps[20]。文献[2]中表明，AUTOSAR 对 CAN-FD 的支持度与推荐度非常高。CAN-FD 具有更快的对象池传输、更低的总线负载使用、更短的最坏情况响应时间和更低的抖动。CAN-FD 的引入是在正确的时间进行的正确的创新，该技术能够跟上汽车以太网技术带来的未来通信机制和网络概念。

2　模型设计

2.1　ECU 安全等级划分

划分 ECU 等级是为了更好地利用总线的资源，使得车载网络通信效率高，时延低，根据　ECU 的安全需求，对数据帧进行 CRC 校验，HMAC 验证或者数据加密。Woo[21]基于汽车安全完整性等级(Automotive Safety Integrity Level，ASIL)设计了 ASL 0-3 四个等级的 ECU 划分方案。同时刘毅[8]也根据 ASIL 规则划分了数据帧安全性等级，但可惜的是 CAN 数据帧的长度限制了安全等级的细节设计。

ASIL 是 ISO 26262 中对车辆进行危害分析与风险评估(hazard analysis and risk assessment，HARA)而得到的对于相关危害进行识别归类的方法。ASIL 制定了四级的程度划分，由低到高分别为 A、B、C 和 D。本研究依据 ASIL 将 ECU 划分如表 1 所示。

ECUs_1 以服务为主的 ECU 节点，包括座椅 ECU、电子仪表盘(EIS)、收音机等和以感知功能为主的 ECU 节点，包括速度感知 ECU、夜视 ECU 等。ECUs_2 以智能决策为主的 ECU 节点，包括信号识别 ECU，轮胎压力监测系统(TPMS)等。ECUs_3 以协同控制为主的 ECU 节点，包括自动变速器控制(ECT)、引擎管理系统(EMS)、自动车身水平控制(ALC)等。ECUs_4 以安全相关功能为主的 ECU 节点，包括安全气囊系统(SRS)、汽车安全辅助系统(SAS)、自动防抱死刹车系统(ABS)等。

表 1　ECU 等级划分

Tab. 1　ECU classification

ASIL 等级	ECU 类型	通信设计	安全等级
A	ECUs_1	Blake2s/2B	NSL0
B	ECUs_2	Blake2s/4B	NSL1
C	ECUs_3	SM4+Blake2s/6B	NSL2
D	ECUs_4	SM4+Blake2s/8B	NSL3

2.2　改进的 PBKDF2

PBKDF2 是 RSA 实验室在 PKCS#5 标准中提出的一种密钥派生函数，该函数基于伪随机函数 HMAC-SHA1 进行多轮迭代，输出不定长度的密码序列。PBKDF2 以其快速与安全性应用于诸多场景，如区块链中的分层确定性钱包，OpenSSL 或其他物联网环境等。但是 PBKDF2-HMAC-SHA1 存在以下问题：

1) HAMC 中的填充计算存在冗余问题。

2) 相较而言，SHA1 存在安全性低的问题，需要足够的迭代次数才可以保证密钥安全性，且低安全度的密钥易被 GPU 阵列或彩虹表破解。

现有的优化方案中，基于硬件的加速，或者基于结构优化的加速[22]，或为了安全性的提升使用 SHA-256 算法等并不适合车联网中计算性能受限的环境和高安全要求，尤其是官方推荐算法迭代轮数达到 10000 次才具备较高的安全性，所以本研究中提出了基于 Blake2s 的改进 PBKDF2 算法，Blake2s-PBKDF2。

Blake2[23]是 SHA-3 决赛的入围者 Blake 的优化版本，其安全性不低于最新标准的 SHA-3，但计算速度快于 SHA-1。所以 Blake2 更适合作为密码哈希算法的伪随机函数(Pseudorandom Function, PRF)[20]，并且 Blake2 在硬件中已可以实现[24]。其中 Blake2s 是 Blake2 针对 32 位平台优化的计算模式，更适合车载系统。在本研究中，本文拟使用 Blake2s 代替 HMAC-SHA-1 作为 PBKDF2 的 PRF 函数，在计算受限的车联网环境中，本算法可以使用更低的迭代轮数实现更高的安全性，同时计算效率更高，同时 Blake2s 可选长度 1 至 32 字节，更适用于分级策略。Blake2s-PBKDF2 伪代码描述如下：

算法 1　Blake2s-PBKDF2

```
输入：Password,Salt,Iterations,Dklen。
输出：DK[0：DKlen]。
a) r = ceil(DKlen/Hlen)。
// 执行块数，Hlen 为 PRF 函数得到的长度，推荐并行程度为 r
b) for 1 to r：T = Blake256(Password, Salt || i)；U = T。
c) for 1 to Iterations：T = Blake256(Password, T)；U =
U XOR T。//此 c)步骤代码在 b)循环中执行
d) DK = DK || U。执行后转步骤 b)
e)return DK[0：DKlen]
```

2.3　ECU 自检

为了防止车辆 ECU 程序中被植入木马，ECU 固件被刷入恶意代码，或者车载网络中被接入非法信息收发设备，所以车载网络的防护中，对 ECU 节点进行认证。Choi[25]利用 CAN 的电信号特性来区分发送方节点，但方案对于 ECU 固件刷新和 ECU 被劫持没有有效的防护。本研究设计了一种在汽车启动时进行 ECU 检测的方案，拟在点火阶段完成 ECU

节点哈希指纹值的验证。汽车启动时 ECU 自检方案如下：

a) 在汽车出厂时，计算各 ECU 节点的固件与软件 hash 值，并将节点 ECU_i 的 hash 值与其 ID，即 EID_i 对应存储在车载 T-Box 中的不可窜改存储介质中。其中 HMAC 表示 Blake2s 算法，EFW_i 表示 ECU_i 的固件软件代码。

$$MAC_i = HMAC(EFW_i \| EID_i) \tag{1}$$

b) 汽车启动时，ECU_i 将自己的软件固件数据和 $ECUID_i$ 经过 CANIF 模块传递和 CANTP 模块封装后，成为 I-PDU 格式，由 PDU Router 转发至 SecOC 模块，SecOC 将该 I-PDU_i 传进 HSM 设备中。HSM 设备将 Blake2s 计算的 hash 值返回至 SecOC。

c)SecOC 将 hash 值经过 RTE 层传递至 T-Box，T-Box 根据本地存储的出厂哈希值对比，若对比通过，则返回 ID 与通过 Flag，若对比失败，则返回 Error 报警信息。

2.4　会话密钥管理

使用固定密钥加密数据并不可取，所以本研究中不使用长期的出厂密钥，在车辆启动时根据车内环境信息的真随机数使用 Blake2s-PBKDF2 算法派生出会话密钥，并设置过期时间(车辆启动至熄火)保存在 HSM 的安全存储介质内。该存储介质只有 HSM 内固定的程序可读，HSM 模块可设置在车载 T-BOX 中，不增加额外硬件成本。汽车启动时密钥生成方案设计如下：

a) 汽车点火启动时，HSM 模块取电池信号特征，选取 128bits 长度为随机序列，选取 16bits 为 salt 值。

b) 调用 HSM 内已经编译好的 Blake2s-PBKDF2 算法模块，计算 DK。其中 BKDF 表示改进的 Blake2s-PBKDF2 算法，random 为随机序列，salt 为盐值，c 为函数内部执行轮数，dkLen 为期望输出的密钥长度。

$$DK = BKDF(\mathrm{random}, \mathrm{salt}, \mathrm{c}, \mathrm{dklen}) \tag{2}$$

c) 步骤 b)中得到的 DK 长度为 256bits，取高 128bits 为车载网络的会话加密密钥(Session Key，SK)，保存在 HSM 的安全存储内。

会话密钥分发需要考虑安全性与效率性，故而文献[8]使用 RSA 证书分发的方式不适用于车载网络，文献[5]的组会话密钥致使经过多轮密钥分发才能通信，文献[7,16]在 SecOC 中添加了数据加密的操作，但存在密钥管理问题。文献[21]设计的密钥分发过程较为复杂，每一个 ECU 都要与网关交互数次，通信量较大。本研究采用与文献[17]相近的 KDC 风格的密钥分发协议。本研究中引入密钥服务器(Key Server，KS)来分发 SK，KS 设置在 T-BOX 中，与 HSM 模块集成。假设需要加密的 ECU_i 与 KS 已预共享密钥 Key_i，Key_i 表示 ECU_i 的长期密钥，存储在 ECU 的安全固件中，KS 的安全存储中存有 ECU 的 id 与 Key 的对照表。

密钥分发步骤如下：

a) KS→ECU_i：KS 将执行式(3)得到结果 send_msg_i，并将其广播至车载网络中。其中 r 为一个随机数，Enc 表示 SM4 算法。

$$send_msg_i = r \| Enc_{Key_i}(SK) \| HMAC(SK \| r) \tag{3}$$

b) ECU_i→KS：ECU_i 接收到 send_msg_i 后，使用密钥 Key_i 解密消息，获取 SK 并验证，验证过后 ECU_i 将执行式(4)得到结果 ack_msg_i 并返回，若验证不通过或未获取密钥，将执行式(5)得到结果 err_msg_i 并返回。其中 EID_i 表示 ECU_i 的 ID 标识：

$$ack_msg_i = Enc_{Key_i}(r+1 \| EID_i) \| HMAC(r+1 \| EID_i) \tag{4}$$

$$err_msg_i = Enc_{Key_i}(r-1 \| EID_i) \| HMAC(r-1 \| EID_i) \tag{5}$$

c) KS 服务器根据 ECU_i 的返回结果决定是否重新执行密钥分发操作。

2.5　ECU 通信流程设计

保护 ECU 通信分为发送端和接收端，本研究中采取符合 SAE J1939 规范的 64B CAN-FD 数据帧格式，符合 J1939 标准的 PDU 格式如图 2 所示。

优先级P 3bits	扩展数据页EDP 1bit	数据页位 DP 1bit	PDU格式 PF 8bits	PDU特定域PS 8bits	源地址SA 8bits	数据域 DATA 64Byte

图 2　PDU 格式图

Fig. 2　PDU format diagram

a) 发送端消息处理过程如下：

(a) ECU 数据帧的层层传递：CAN Driver 收取 ECU 的报文生成 L-PDU，L-PDU 进入 CAN Interface 进行抽象处理成为 N-PDU，N-PDU 进入 CAN Tp 生成 I-PDU，PDUR 模块将需要添加认证的 I-PDU 路由至 SecOC 模块。

(b) SecOC 模块初始化缓存区后识别 PDU 中的源地址，判断该发送端 ECU 属于 NSL0-3 这四个级别中的那个级别，并分别执行对应的操作以生成 MAC 或者密文：

NSL0 和 NSL1：此级别中的数据帧需要添加 MAC 码以保证其完整性检验，在本研究中，使用更加快捷的 Blake2s 计算。SecOC 将以下数据传输至连接的优化固件的 HSM 中：I-PDU 的标识符 ID，ECU 数据和完整的新鲜度值，HSM 接收这三个数据之后，HSM 使用以下公式计算 MAC 码。其中 PID_i 为该 PDU 标识符，$DATA_i$ 为 PDU 中携带的数据，FV 为完整的新鲜度值，dklen 为期望得到的长度，此处为 2 或者 4。

$$\mathrm{Authenticator} = HMAC(\mathrm{PID_i} \| \mathrm{DATA_i} \| \mathrm{FV}, \mathrm{dklen}) \tag{6}$$

NSL2 和 NSL3：此部分的 Secured I-PDU 构建过程中需要保护数据防窃取，与上述步骤中不同的是，Blake2s 期望得到的长度不一，ECU 需要先执行 SM4 加密算法得到加密的数据，将密文和 MAC 传输至 SecOC 模块。式(6)中的 dklen 分别为 6 或 8。

$$Cipher = Enc_{SK}(DATA_i) \tag{7}$$

$$Authenticator = HMAC(PID_i \| Cipher_i \| FV, dklen) \tag{8}$$

(c) SecOC 中新鲜度值管理器(Freshness Manager，FVM)提供接口收发字节数组形式的新鲜度值，在本研究中，新鲜度值以计数器的形式出现，并将新鲜度值截取长度设置为 8，所以在 secured I-PDU 构建的过程中，将截取新鲜度值的低 8bits 作为参数添加在报文中。只有当 SecOC 调用 PduR 模块进行进一步路由时，该新鲜度值计数器递增。

(d) 缓存区将按照如下公式构造 Secured I-PDU：

$$\begin{aligned} &SecuredIPDU = \\ &SecurredIPDUHeader \| Cipher \| TruncatedFV \| Authenticator \end{aligned} \tag{9}$$

(e) 当缓存区中构造完成 Secured I-PDU 后，SecOC 模块将 Secured I-PDU 交由 PduR 路由(此时计数器递增)。

b) 接收端消息处理过程如下：

(a) SecOC 为每一个 Secured I-PDU 维护一个验证构建计数器(Authentication Build Counter，ABC)和验证尝试计数器(Authentication Verify Attempt Counter，AVAC)，并设初始值为 0。这两个计数器将参与整个 Secured I-PDU 验证过程。FVM 接收来自 Secured I-PDU 的新鲜度值，在内部查询：若查询后无返回结果，则 ABC 递增，不执行验证尝试，反之返回值为可恢复错误如工作栈忙碌等，则 ABC 递增；若验证构建失败，且 ABC 未达到阈值，则重新刷新验证过程；若验证构建成功，但验证失败，譬如 MAC 验证不通过，AVAC 递增，ABC 置为 0；若对新鲜度函数的查询返回一个不可恢复的错误，譬如新鲜度配置导致的系统故障，或者 ABC、AVAC 达到阈值，SecOC 都将此 Secured I-PDU 移出验证缓存区并丢弃；若验证通过，返回类型将被设置为 SECOC_VERIFICATIONSUCCESS。

(b) SecOC 模块将按照如下方式去构建验证所需的新鲜度值(FreshnessVerifyValue，FVV)：由于本研究使用截断的新

鲜度值，所以直接从非完整传输的构建方案开始，首先，AVAC 将递增，接着对比新收到的 Secured I-PDU 中的截断新鲜度值(NewFreshnessValue，NFV)与上次验证的新鲜度值(Old FreshnessValue，OFV)，若 NFV 大于 OFV，则 FVV=OFV hign bits || NFV，反之 FVV=OFV hign bits+1 || NFV，如此验证所需的新鲜度值便构建完成

(c)加密过的数据将由 ECU 自行解密，解密步骤在 MAC 验证通过之后。计算公式如下，其中 Dec 为 SM4 的解密算法。

$$DATA=Dec_{SK}(Cipher) \tag{10}$$

(d) SecOC 模块为 MAC 验证构造数据，与 MAC 生成过程一致，SecOC 模块通过将 DataToAuthenticator 及其长度与从 Secured I-PDU 解析的 MAC 及其长度传递到对应的认证算法中来验证 MAC，在 HSM 中完成验证的计算操作。

$$\text{DataToAuthenticator}=(PDUID_i \,\|\, DATA_i \,\|\, FVV, \text{dklern}) \tag{11}$$

(e) 验证模块验证该 Secured I-PDU 的 MAC，若根据传递的数据计算出的验证 MAC 与 Secured I-PDU 的 MAC 对比一致，则返回验证正确结果，若验证不通过，则分以下两种情况，第一种为 AVAC 达到阈值，则直接丢弃该帧，第二种为 AVAC 未达到阈值，则 AVAC 与 FVV 都递增，再次执行 MAC 验证操作。

(f) SecOC 需要将返回的验证结果传递给 FVM，将该数据帧传递到上层应用或对应的 ECU。

3　安全与性能分析

3.1　安全分析

本章节对基于 SecOC 的车载网络安全通信模型的安全性进行形式化分析。

1) 设 E1、E2、E3 和 E4 分别为 2.1 节中分类的 ECUs_1 至 ECUs_4 的 ECU 集合，则模型中的总 ECU 集合为 E==E1∪E2∪E3∪E4，则声明对象 e1,e2:E，(e1,e2)∈E╳E。

2) 设 ECU 的 id:ID，ECU 哈希指纹集合 H，则存在 ECU 与其对应的哈希指纹表{id:ID;h:H}，(id,h)∈ID╳H。

3) 设新鲜度值集合 FV=={x:Z|0<x≤max}，声明对象 fv:FV。

4) HSM 中已存储密钥 k。

定理 1　ECU 安全，修改固件或外装的 ECU 被检测出来

证明　假设现有一个被注入恶意代码、修改固件程序或者后装的 ECU_fake 在汽车内部已存在，在点火时经过 HSM 计算将指纹 h_fake 发送至 T-BOX 验证，(id,h_fake)≠(id,h)或者 id!∈ID∧h_fake!∈H，验证不通过则报警。

定理 2　抗重放攻击

证明　假设车载网络中有一中间者监听到一个报文后多次放入网络。接收端将报文放入 S　ecOC 模块验证，重放报文的新鲜度值为 fv_fake∈N，从 FVM 中接受的新鲜度值为 fv∈N，在 MAC 验证过程中 MAC_fv_fake≠MAC_fv，验证失败，此报文被丢弃。

定理 3　抗窜改报文欺骗

证明　假设车载网络中有一中间者截获一个报文，将报文中载荷的 DATA 域数据部分修改后重传入网络，接收端验证报文时，DataToAuthenticat_data_fake≠DataToAuthenticat，Blake2s 计算出的 MAC 不等，验证不通过丢弃此报文。

定理 4　抗信息窃听

证明　假设车载网络中有一中间者要窃取汽车信息，截获关键 ECU 或系统的报文，本研究中关键数据已使用 SM4 加密，En(k,Data)，因为密钥在 HSM 安全区，中间者无法获取该信息。

定理 5　密码算法安全

证明　本研究中使用的 SM4 的 S 盒的表达中多项式为 254 次、255 项，具有最高的复杂度，根据差分密码分析、线性密码分析、多维线性密码分析等过重密码分析技术测试，SM4 拥有足够的安全冗余度。文献[24]表明，Blake2 对旋转密码分析、迭代差分分析和不可能差分分析等具有一定的抗性与安全冗余度。

定理 6　密钥安全

证明　本研究中的会话密钥在车辆启动至熄火期间有效，128 位的密钥破解复杂度为 2^{128}，故而会话密钥安全。主密钥安全性可使用 VulCAN[12]中的 Sancus[26]结构，使用受保护模块(Protected Module Architectures，PMAs)保护主密钥安全。PM 内存只能通过特定代码段访问，该代码段只能通过单个入口点输入，拥有高安全性和高效性，且成本低廉不增加设备。

3.2　性能分析

在 Linux 5.4 内核，4G 运行内存下，软件测试 SHA-256、Blake2s-256、改进 HMAC 的 PBKDF2 与 Blake2s-PBKDF2 计算效率如表 2 所示，相同条件下，Blake2s 和基于 Blake2s 改进的 Blake2s-PBKDF2 拥有更好的计算效率。

表 2　软件环境中的效率测试

Tab. 2　Efficiency testing in software environment

执行轮数	SHA-256 /ms	Blake2s-256/ms	改进 HMAC 的 PBKDF2/ms	Blake2s-PBKDF2/ms
1000	0.3	0.07	1	0.2
10000	1.8	0.4	3	1
100000	15.9	3.6	27	10

将本研究中提出的基于 SecOC 的车载网络安全通信模型与现有模型对比，本文提供了更全面的安全保障，如表 3 所示。

表 3　基于 SecOC 的安全模型对比

Tab. 3　Comparison of security models based on secoc

模型	ECU 划分	消息加密	MAC	ECU 认证	密钥管理
文献[4]	无	无	CAMC-AES	无	无
文献[6]	无	无	CAMC-AES	无	初始化写入 ECU
文献[7]	DataID	AES	CMAC-AES/2B	无	根据数据从本地密钥库更新
文献[13]	ASIL	无	CMAC-AES/2B	无	初始化写入 ECU
文献[10]	无	无	CMAC-AES/2B	无	初始化主密钥、软件生成会话密钥
文献[12]	无	无	CMAC-AES/2B	基于主密钥认证	初始化主密钥、AS 软件分发会话密钥
文献[17]	无	AES	HMAC-SHA/8B	基于主密钥认证	初始化写入 ECU、SKDC 分发会话密钥
文献[9]	DataID	无	CMAC-AES/28bit/44bit	无	初始化写入 ECU
本文	ASIL	SM4	Blake2s	指纹值	BKDF 生成、KS 分发

4　结束语

本研究分析并总结现有国内外基于 SecOC 的车载网络保护模型的不足之处，提出一种基于 SecOC 的车载网络安全通信模型，模型中根据 SAIL 将 ECU 划分不同的安全等级，更好地利用车载网络资源；基于 Blake2s 改进现有的 PBKDF2 算法，在启动阶段使用车载环境的真实物理参数衍生出会话密钥，并存储在 HSM 模块中，在驾驶期间有效；在点火阶段验证通电 ECU 的哈希指纹值，在通信阶段使用 SM4 加密通信数据，Blake2s 生成可选长度的 MAC 消息验证码。通过实验和分析证明，该模型计算效率高，并提供更全面的安全保护，符合中国信通院提出的由内而外地保护车联网安全要求。

密钥管理是加密模型中最重要的一环，相比于通过会话破解密码，直接从设备中获取密钥是更快捷的方式，所以在

车载环境中设计加密步骤，需要着重考虑密钥管理方案。故而本研究中密钥管理将是下一步研究的重心，进一步优化密钥的生成，存储和使用。

参考文献：

[1] 吴武飞，李仁发，曾刚，等．智能网联车网络安全研究综述 [J]. 通信学报，2020, 41 (6): 14. (Wu Wufei, Li Renfa, Zeng Gang, *et al.* Summary of research on network security of intelligent network connected vehicles [J]. Journal of communications, 2020, 41 (6): 14)

[2] Specification of Secure Onboard Communication. AUTOSAR_ SWS_Secure Onboard Communication [EB/OL]. 2020. https://www. autosar. org/

[3] 余其涛．基于 AUTOSAR 标准的 CAN 通信栈设计与实现 [D]. 上海交通大学，2016. (Yu Qitao. Design and implementation of CAN communication stack based on AUTOSAR standard [D]. Shanghai Jiaotong University, 2016.)

[4] 吴志红，李清晨，朱元，等．AUTOSAR 规范下安全车载通信技术的研究与实现 [J]. 通信技术，2017, 50 (12): 2822-2827. (Wu Zhihong, Li Chenchen, Zhu Yuan, *et al.* Research and implementation of safety vehicle communication technology under AUTOSAR specification [J]. Communication technology, 2017, 50 (12): 2822-2827)

[5] 罗峰，胡强，刘宇．基于 CAN-FD 总线的车载网络安全通信 [J]. 同济大学学报：自然科学版，2019, 47 (3): 386-391. (Luo Feng, Hu Qiang, Liu Yu. Vehicle network security communication based on can-fd bus [J]. Journal of Tongji University: Natural Science Edition, 2019, 47 (3): 386-391)

[6] 黄大权．车联网安全通信技术的研究与实现 [D]. 电子科技大学，2019. (Huang Daquan. Research and implementation of secure communication technology for Internet of vehicles [D]. University of Electronic Science and technology, 2019)

[7] 罗超．面向联网汽车车内网络的防御技术研究与实现 [D]. 电子科技大学．2020 (Luo Chao. Research and implementation of Defense Technology for in vehicle network of networked vehicles [D]. University of Electronic Science and technology. 2020)

[8] 刘毅．基于车载 CAN 总线网络的安全协议研究 [D]. 吉林大学，2019. (Liu Yi. Research on security protocol based on vehicle can bus network [D]. Jilin University, 2019)

[9] Böhner M, Mattausch A, Much A. Extending software architectures from safety to security [J]. Automotive Safety & Security 2014, 2015.

[10] Radu A I, Garcia F D. LeiA: A lightweight authentication protocol for CAN [C]// European Symposium on Research in Computer Security. Springer, Cham, 2016: 283-300.

[11] Nyurnberger S, Rossow C. –vatican–vetted, authenticated can bus [C]// International Conference on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2016: 106-124.

[12] Van B J, Myuhlberg J T, Piessens F. VulCAN: Efficient component authentication and software isolation for automotive control networks [C]// Proceedings of the 33rd Annual Computer Security Applications Conference. 2017: 225-237.

[13] Wu Z, Zhu Y, Lei X, *et al.* Functional safety and secure CAN in motor control system design for electric vehicles [R]. SAE Technical Paper, 2017.

[14] Rosenstatter T, Sandberg C, Olovsson T. Extending AUTOSAR's Counter-Based Solution for Freshness of Authenticated Messages in Vehicles [C]// 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC) . IEEE, 2019: 1-109.

[15] Rosenstatter T. Towards a Standardised Framework for Securing Connected Vehicles [M]. Chalmers Tekniska Hogskola (Sweden) , 2019.

[16] Bella G, Biondi P, Costantino G, *et al.* CINNAMON: A Module for AUTOSAR Secure Onboard Communication [C]// 2020 16th European Dependable Computing Conference (EDCC) . IEEE, 2020: 103-110.

[17] Xiao Y, Shi S, Zhang N, *et al.* Session Key Distribution Made Practical for CAN and CAN-FD Message Authentication [C]// Annual Computer Security Applications Conference. 2020: 681-693.

[18] Yalçın S B, Soltekin M M E. Designing and Implementing Secure Automotive Network for Autonomous Cars [C]// 2021 29th Signal Processing and Communications Applications Conference (SIU) . IEEE, 2021: 1-4.

[19] 胡嘉航．硬件安全模块的设计及应用 [D]. 杭州电子科技大学．(Hu Jiahang. Design and application of hardware security module [D]. Hangzhou University of Electronic Science and technology)

[20] Kang S, Seong J, Lee M. Controller area network with flexible data rate transmitter design with low electromagnetic emission [J]. IEEE Trans on Vehicular Technology, 2018, 67 (8): 7290-7298.

[21] Woo S, Jo H J, Kim I S, *et al.* A Practical Security Architecture for In-Vehicle CAN-FD [J]. IEEE Trans on Intelligent Transportation Systems, 2016: 2248-2261.

[22] Visconti A, Gorla F. Exploiting an HMAC-SHA-1 optimization to speed up PBKDF2 [J]. IEEE Transactions on Dependable and Secure Computing, 2018, 17 (4): 775-781.

[23] Aumasson J P, Neves S, Wilcox-O'Hearn Z, *et al.* BLAKE2: simpler, smaller, fast as MD5 [C]// International Conference on Applied Cryptography and Network Security. Springer, Berlin, Heidelberg, 2013: 119-135.

[24] Atiwa S, Dawji Y, Refaey A, *et al.* Accelerated hardware implementation of blake2 cryptographic hash for blockchain [C]// 2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) . IEEE, 2020: 1-6.

[25] Choi W, Jo H J, Woo S, *et al.* Identifying ecus using inimitable characteristics of signals in controller area networks [J]. IEEE Trans on Vehicular Technology, 2018, 67 (6): 4757-4770.

[26] Noorman J, Freiling F, Bulck J V, *et al.* Sancus 2. 0: A Low-Cost Security Architecture for IoT Devices [J]. ACM Transactions on Privacy and Security, 2017, 20 (3): 1-33.